List of Dissertation Abstract （Information Media and Environment Sciences　Information Media Course）

Name	Supervisor	Title	Abstract
Tomoo OSHIKA	Junji SHIKATA	High-functional encryption from Identity based homomorphic encryption	Along with the development of network technology, emphasis is not only safety but also functionality. Homomorphic encryption which allows computation on ciphertexts, generating an encrypted result, when decrypted, result of the operations had been performed on the plaintext. I studied whether homomorphic can have various other functions at the same time.
Yao XIAO	Katsunari YOSHIOKA	A Study on Analysis of Social Engineering of Targeted Email Attack	In recent years, targeted attacks that send malware-attached mails to the target have been increasing. When the attached file is opened, it shows a decoy document that is relevant to the target in order to conceal the infection. We collect decoy documents to infer the targeted individuals or organizations.
Zhiyong YANG	Katsunari YOSHIOKA	Observation and Analysis of Cyber Attacks in Home Network	Recently the number of connected devices is increasing rapidly. While these IoT devices receive large benefits from diverse services provided via Internet, there is a concern about cyber attacks against them. Nevertheless, investigations and researches on cyber attacks in home networks are surprisingly few and unexplored. In this study, we develop a home network testbed and test proof-of-concept attacks that could potentially be conducted against these devices in home network and observe their effect. Finally, we discuss the framework to evaluate home network security products.
Ryohei AKUTSU	Katsunori OKAJIMA	Visibility evaluation formula considering contrast polarity of text and age of observer	By conducting the experiment presenting text with different contrast polarity conditions and getting its subjective visibility, we found the visibility evaluation formula integrating contrast polarity of text. Also, we analyzed the formula and revealed characteristics and limitation related to character size. Finally, experiment conducted for elderly people. Results suggested “contrast polarity effect” occurred by hazy media. Considering this effect and the age-related decline in contrast sensitivity, the visibility evaluation formula for the elderly people was obtained, which can evaluate the visibility of both contrast polarity conditions.

Akihiro IIZUKA	Tatsunori MORI	A study on retrirval method of passage related to given key-phrases in essay-type examinan of world histry	In this research, the search unit in the automatic answer system of the University of Tokyo entrance examination world history, the use of the query decomposed into the constituent words of the specified phrase and the pseudo relevance using the search query extension by the feedback of the passage acquired by the search. We proposed a feedback method. As a result of the evaluation experiment, recall rate in search was improved by giving information on passages related to specified phrases.
Kohei IIZUKA	Tomoharu NAGAO	Automatic Construction of Image Feature Quantity Extractor Focused on Analytical Property	In this paper, the authors propose an automatic construction method of image feature quantity extractor with emphasis on analytical property. Proposed model is based on automatic construction of tree structure image transformation (GMA) and feature quantity extractor (SIFTER). We conduct comparative experiments on the method and accuracy that restricted functions. Experimental results show that the proposed system is effective.
Kota ISOBE	Takashi TOMII	An Estimation System of EV Energy Consumption for Driving on Unexperienced Roads	In this paper, we construct a system that estimates the energy consumption of electric vehicle (EV) driving on roads without driving experience. To travel without worrying about running out a battery, EV users need to prepare a driving plan based on energy consumption in advance. To solve this problem, we calculate to plan by finding the minimum/maximum power consumption from the simulation when an EV travel the registered route. With this plan, once it is possible to know the limit spot where we can reach and the place where there is a possibility of running out a battery. To evaluate this system, we conducted driving EV experiments and verified the estimation accuracy of EV's energy consumption.
Yuki ITO	Tomoharu NAGAO	Harvest Maximization at Plant Factory using Bayesian Optimization	Plant factories need to increase their harvest, but it takes many days in plant grows. In this paper, we propose improving method to limit sampling area in Bayesian optimization for such expensive functions. With the benchmark functions experiment, our method seemed to update the optimal solution frequently, and finally found better solution than the original. In addition, we applied our method to harvest maximization problem and could found the settings which we can grow lettuce heavier in dry weight by 40% with than expert ones.
Ryuhei IBARAKI	Takashi TOMII	Construction of Energy Life-Log DB for Considering the Introduction Effect of Smartgrid	In this research, we construct a consolidated database that accumulates energy life logs with unified time granularity, and applies it to the simulation of energy balance in smart grid. In this paper, we analyze the energy balance according to the introduction amount of the components of the smart grid by using real data, and showed that the integrated database is useful for examining the introduction effect of smart grid.

Wataru UENO	Katsunari YOSHIOKA	A Study on Countermeasure of Malware that Evade Security Analysis	Recently, in order to cope with increasing cyber-attacks, the defender makes use of analysis system such as honeypot, a decoy system to monitor and analyze cyber attacks. However, it has been reported that attackers detect analysis systems with various ways and evade their analysis. Therefore, in this paper, we investigate, implement, and evaluate evasion-resilient cyber-attack analysis system.
Tadahiro UCHIKOSHI	Junji SHIKATA	A Study on Construction of Advanced Cryptographic Protocols Based on a Framework of Hybrid Encryption	In this thesis, we construct cryptographic systems with advanced functionality based on the KEM/DEM framework. Specifically, we construct Forward Secure PKE and Anonymous Broadcast Encryption based on the KEM/DEM framework, and analyze requirements of KEM and DEM so that the resulting systems are secure. As a result, we show that if the underlying KEM has an advanced functionality, then the resulting system can inherit its functionally.
Masahiro EBINA	Junji SHIKATA	Study on Efficient Threshold Public-Key Encryption from a Weak Complexity Assumption.	A Public-key encryption is based on any complexity assumption. It is one of important research directions to design from the weakest possible complexity assumption. In my thesis, we propose an efficient threshold public-keyencryption system secure against chosen ciphertext attacks from the hard search problem. Furthermore, we show the construction for making some parameter length more efficient and compare it with previous works.
Kenya OKUTOMI	Tsutomu MATSUMOTO	A Study on Tamper Resistant Hardware for Advanced Encryption Standard and Pairing Based Cryptography	In recent years, cryptographic techniques have been used for various information devices to protect the information and communication contents therein. However, side-channel attacks using physical information for information equipment pose a threat. The term "tamper resistance" which indicates difficulty in deciphering information equipment is used. In order to improve the tamper resistance, we will consider attack methods that can pose new threats to the currently used AES and pairing-based cryptography expected to be used in the future.
Rina KATO	Katsunari YOSHIOKA	A Study on Honeypot Imitating a Remote Monitoring and Control System Deployed in Infrastructure Facilities	We built the honeypot imitating a remote monitoring and control system using the real data logger and PLC, and observed accesses to the honeypot. As a result, we observed accessors who do not hesitate to carry out highly aggressive operations, and those who seem to be aiming for investigation.

Yoshihisa KANOU	Tomoharu NAGAO	Generation of Continuous Facial Expression Space without Emotional Labels	When handling facial expressions in machine learning, it is necessary to give labels which are teacher signals to facial expressions. However, from the viewpoint of cost of building a dataset, one-hot labels attached to emotions are given, and the continuity of facial expressions is often not considered. In this research, we propose a method to generate face expression space by learning the continuity of facial expressions separated from subject-specific features as latent spaces inside the model without using labels on facial expressions. In the experiment, visualization of latent space, image generation, and unsupervised facial expression classification task are conducted, and we verify the effectiveness of the separated subject feature / facial expression feature and facial expression space
Yusei KAWAI	Shinichi SHIRAKAWA	Dynamic Selection of Image Processing Filters for Convolutional Neural Networks	Convolutional neural networks (CNNs) show remarkable performance on image recognition tasks. Several studies report that the preprocessing by ordinary image processing filters helps to improve the performance of CNNs. However, the selection of appropriate filters depending on datasets requires trial-and-error or huge computational cost. This thesis proposes an efficient automatic selection method of preprocessing filters by optimizing the probabilistic distribution for the filters during the model training. The experiment using several datasets shows that the proposed method can contribute to improving predictive performance.
Daiki KOUNO	Katsunori OKAJIMA	Effects of color and visual cloudiness on evaluation of beverage	There are many studies on the cross-modal effects of the color of the beverage, but there is no study on the cross-modal effects on cloudiness of the beverage. Therefore, in this study, we conducted experiments on the influence on the evaluation of the taste when changing the cloudiness as well as color of the beverage with AR. As a result, it was possible to increase bitterness of green tea and fruitiness of fruit beverages due to visual cloudiness of the beverage, where as it was suggested when the visual cloudiness was too high. That the evaluation would be lowered.
Shota SAITO	Shinichi SHIRAKAWA	Dynamic Structure Optimization with Regularization for Controlling Model Complexity of Deep Learning	Deep neural network (DNN) is a major machine learning model, which shows remarkable performance on various tasks, such as image recognition. Deploying to the limited computing resources, such as smartphones, a memory efficient yet well-performed structure is required. This thesis focuses on a method that simultaneously optimizes the weights and DNN structure by using the probabilistic model of the structures and introduces a penalty term based on the model complexity into the objective function to control the model complexity. From the experiment of connection selection in DNN for image classification, the proposed method succeeded in reducing the number of weights by about 60% while keeping the increase of the classification error rate within 1%.

Yusuke SAITO	Takashi TOMII	Accuracy Evaluation to Estimate Energy Consumption for EV Energy Life Log Database	We have run ECOLOG that estimates the energy consumption when driving in an EV with sensor data and stores it in the database as an EV Energy Life Log. In this paper, we verified the accuracy of the EV energy consumption model in the ECOLOG. We applied cleansing to the data used for verification. As a result, the accuracy of the estimation model is improved.
Ro SAITO	Naoyoshi TAMURA	Exercise-Song Proposal System Research For Supporting Guitar Practice	Instrumentalists feel the difficulty when they play instruments such as the guitar, however it has not been cleared that the difficulty depends on which elements of songs. Our target is revealing the relationship between score and difficulty in terms of score statistics, over and above applying it to exercise-song proposal system. In this research, we clarified 4 factor “fingering”, “frequency”, “rhythm”, and “speed” affect difficulty and enabled to calculate the difficulty from a score by analyzing evaluation scale of guitar players.
Satoru SAKURAZAWA	Tsutomu MATSUMOTO	A Study of Instrumentation Security Evaluation System for ToF Depth-Image Cameras	The security on sensors - "Instrumentation Security" is important for Cyber Physical System which takes information on physical space into cyber space and applies the processing result to physical space. In this paper, I show that I constructed a system to evaluate instrumentation security for ToF depth-image cameras which are 3D distance sensors by executing the measurement pulse spoofing as the simulation attack. Furthermore, I show the evaluation results for the ToF depth-image cameras which are on the market.
Takuro SAWADA	Katsunori OKAJIMA	Temporal characteristics of impression judgment and hierarchy of the brain mechanism	In this research, I focused on the tachistoscopic impression judgment. We presented various images tachistoscopically and evaluated "brightness" "beauty" and "preference". As a result, it showed that brightness perception and charm perception had mutual influence. We also suggested that feedback processing of charm perception may affect brightness perception. From the results of the experiment, we proposed hierarchy of the brain mechanism of impression judgment in which feedback and feedforward processing of brightness and attraction perception are performed.
Seiya SUZUKI	Tatsunori MORI	A study of a method for Extraction of cited texts in Web documents	This study proposes a method to extract cited texts in Web documents. And it aims to complete the entire extraction of source information in Web documents (in this study, source information means a pair of cited texts and source tests), with previous study.

Ryota TANAKA	Junji SHIKATA	A Study on Encoding Methods for Data Privacy and Authenticator Compression	With the spread of IoT devices and the evolution of computers, information traffic has dramatically increased. There are research areas of encryption and authentication techniques based on coding theory. In this thesis, for data privacy, we propose Wiretap Channel II with an active eavesdropper and derive upper and lower bounds of secrecy rates. In addition, for authenticator compression, we propose construction of aggregate MACs with tracing based on bi-orthogonal justification data compression codes.
Kazuki TAMIYA	Katsunari YOSHIOKA	A Study on Observation and Countermeasure of Cyber Attacks Using Real IoT Devices	Cyber attacks against IoT devices are increasing in recent years. In this research, we conducted research from two viewpoints of "observation" and "countermeasure" of cyber attacks on IoT devices. In the research on "observation",I observed and analyzed the IP camera's peeping using decoy IP camera. In the research on " countermeasures" , We proposed IoT malware removal and infection prevention method and verified its effectiveness by using real devices.
Moeka NAKAJIMA	Katsunori OKAJIMA	Effects of emotional strength and face direction in facial emotion recognition	Previous studies on facial expression recognition have not considered the facial direction and the strength of the emotion. We conducted visual perceptual experiments as a function of facial direction and found that the expression recognition performance decreases when the angle of the face deviates from the frontal position. In addition, we found that the accuracy of emotion recognition of side faces increases after visual perceptual learning. Finally, we conducted an experiment using stimuli morphed from neutral to each basic emotion. The results showed that observers felt the emotion strongly when the facial landmarks are close to the basic emotion positions.
Shin NISHIDA	Katsunari YOSHIOKA	A Study on Notification to users of IoT devices with security flaws	Notification of vulnerability and malware infection of IoT devices to the stakeholders is becoming increasingly important. Therefore, various studies have been conducted to measure and compare the effectiveness of notifications in various setups. In this study, we focus on a case in which notification can be done via dedicated client software installed on users PCs and/or smart phones. We show a design for notification experiment particularly for WarpDrive project.

Shimpei NISHIMURA	Tomoharu NAGAO	Introduction of Escapism as Intrinsic Motivation to Reinforcement Learning	In this paper, we model escapism, one of the elements of intrinsic motivation, and propose a method to improve learning performance of agents' policy by applying the model to reinforcement learning. Our model of escapism consists of the concept of stress and learning-task switching based on stress. To examine effectiveness of the proposed model, we trained agents in the simulation environment. The results showed that reinforcement learning with the proposed model outperformed naive reinforcement learning. Furthermore, we also confirmed that our model was equivalent to previous model on intrinsic motivation in terms of learning performance.
Hiroki NOHIRA	Tsutomu MATSUMOTO	A Study on Instrumentation Security of Stereo Vision Camera	Stereo vision cameras are used in human life related systems or systems with a lot of financial damage if it cannot run. Therefore, it can be said that raising instrumentation security of stereo cameras has social significance. In this paper, we identify the instrumentation principle of the stereo vision camera and the composition of its implementation, and show what kind of attack can be considered from the components of each implementation. Then demonstrate that the attack is a threat. Furthermore, we will use it in establishing the evaluation method of the instrumentation security of the stereo camera from the examination result of the attack method.
Yuta HAMASAKI	Takashi TOMII	A Visualization System of Parallel Coordinate Plots Integrating Multivariate Data by SPJ Query	Presently, all the multivariate data can be accumulated due to the development of sensor / storage device technologies and the publication of open data. However, it is generally difficult to analyze multivariate data, so support of a visualization system is indispensable. In this paper, we present a visualization system of parallel coordinate plots extended by SPJ Query and operation snapshot. In addition, we show availability of the proposed system by demonstration of Kosode Byobu and a car traveling log.
Chiaki HIRAYAMA	Tomoharu NAGAO	Alleviating Congestion of Swarm Transfer Robots using Classifier System	Congestion alleviation and transfer time reduction of swarm transfer robots have been attracted attention as the systems have been introduced to the real world, like logistic centers. To select paths which can decrease congestion, we propose the dynamic Dijkstra’s algorithm that path-costs are updated based on surrounding conditions of fixed points. We use Classifier Systems to get dynamic path-cost update rules. Compared to a previous approach, the proposed method decreased by 2.9% average transfer time and more than 7% max transfer time.

Yuta FUKUHARA	Tatsunori MORI	Utilization of historical timeline by country in question answering system to solve world history essay	In recent years, question answering research for world history essay in university entrance exam become active. Previous research to solve this questions retrieve textbooks,but has a problem that the proposed method can't get required text in answer.Therefore, we propose using historical timeline by country and getting required text exhaustively.
Takuya HOIZUMI	Katsunari YOSHIOKA	A study on discrimination of user environments using network scan	In recent years, cyber attack targeting insecure IoT devices has become a great threat. It is believed that one of the root causes is the lack of users' awareness on the device security. In this research, we propose a method to grasp the security status of network devices owned by several hundreds of voluntary users of a security project by clustering the results of network scans on their devices.
Ryo MIYACHI	Tsutomu MATSUMOTO	A Study on Tamper Resitant Implementation for Post-Quantum Cryptography	In order to realize a quantum computer, post-quantum cryptography has attracted attention. In particular, Ring-LWE cryptosystems are more often implemented on embedded devices because of their higher efficiency than other methods. There is a possibility that security of the system may be lost due to vulnerability based on cryptographic implementation method when cryptography is operated by small and medium-sized nodes on the network In this research, side-channel security evaluation is carried out with the aim of tamper resistant implementation for post-quantum cryptography.
Takeshi MORIMOTO	Tatsunori MORI	The Improvement of Recognition Error of the Way of Extracting Onomatopoeia and Presumption of their Impressions	Onomatopoeia is important in Japanese communication. Though identifying position of onomatopoeia in sentences and presuming their impression is essential for workers engaged in onomatopoeia research and Japanese language learner, the way of automating their processes isn't perfect. So we propose the way of improving their problems.
Kenichi YAMADA	Junji SHIKATA	A Study of Fuzzy Extractor with Robustness and Small Entropy Loss	A fuzzy extractor converts non-uniformly source into uniformly distributed output, and it is required to have small entropy loss which is the difference between the entropy of the source and the entropy of the output. A robust fuzzy extractor is a fuzzy extractor which can detect manipulation of the helper strings. In this thesis, we propose a new robust fuzzy extractor under the assumption that we can know a source distribution and show the entropy loss of our extractor is smaller than those of any previous ones.

Shinichiro YOSHIZAWA	Tomohiro FUZII	Defeasibility of scalar implicatures	This thesis discusses scalar implicature and its defeasibility. Gazdar (1979) proposed a theory of generation and cancellation of scalar implicatures, which was intended to predict when implicatures are generated and when they get cancelled. Levinson (2000) discussed one example, which he argued the Gazdar theory cannot account for. The thesis reexamines Levinson's argument and attempts to show it is possible to modify Gazdar's theory in a way that allows it to accommodate the example, though Levinson himself didn't discuss such a possibility. Then, it is observed that the modified version of the Gazdar theory cannot be a real solution to the problem. The observation provides new empirical support for Levinson's original position.
kazuya WAGA	Tatsunori MORI	A method using topic analysis for estimating things in the background of short document	Microblogging is a popular media for users to send information easily. Owing to its characteristics, there are many short document .And sometimes it does not make it clear about things in the background of document. In this research, we consider a method to estimate things behind short document information. We propose a method doing a Web search by use of words contained in the sentences and narrowing down candidates of background things by topic analysis.
Ekaterina EREMEEVA	Tomohiro FUJII	Aspects of positive and negative politeness in Japanese	In this master's thesis, I address the issues of positive and negative politeness in Japanese. I discuss such works as Brown and Levinson (1987) and Matsumoto (1988), looking into applicability of Brown and Levinson's theory to Japanese as well as Matsumoto's objections to it. I attempt to dismantle Matsumoto's analysis of relationship-acknowledgement devices (RAD) in Japanese. Further on, I perform an analysis of the two common Japanese politeness phenomena (sumimasen, analyzed as an instance of negative politeness here, and sentence final particle ne, analyzed as an instance of positive politeness here) that, in my view, support Brown and Levinson's claims about universality of face.
Zhengnan XIA	Katsunori OKAJIMA	The Influence of Audition on Wind Sense and the Determination Mechanism of Wind Strength	Since humans use audition and wind sense when feeling the wind, the multi-modal phenomena always occurs, but it is not known whether the cross-modal phenomenon occurs. In this study, we examined the influence of audition on wind sense, and confirmed that the cross-modal phenomenon occurs when feeling the wind. Furthermore, we formulated the "feeling of wind strength" etc. Based on the results of this research, it is possible to control the "feeling of wind strength" by changing only the wind sound, so it can be expected to be applied to movie theaters and VR systems where high realism is required.

Bingqing DU	Tomoharu NAGAO	Similarity Computation for Drawing Images Using Deep Learning	To solve a drawing similarity retrieval problem, Text-Based Image Retrieval (TBIR), in which keywords are previously attached to the images, is widely adopted. Using TBIR enables narrowing down the retrieval result candidates, while Content-Based Image Retrieval (CBIR), which uses image information instead of text information, is able to narrow even further. This thesis argues image similarity retrieval methods for patent drawings. Considering the huge amount of the image data provided by the patent drawings accumulated for decades, methods adopting Deep Learning (DL) models are considered, and this thesis attempts to find out a DL model enabling similarity compute between drawings in a variety of classes.
Jia XIONG	Katsunari YOSHIOKA	Experimental Analysis of Threats in the Home Network	Recently the number of connected devices is increasing rapidly. With the advent of malware aiming at these devices, many IoT devices are infected and become problematic. In this study, we do the experimental analysis of threats in the home network and we discuss how to build malware sandboxes using real IoT devices and investigate the adequacy of five devices for such purpose. We also present the result of analyzing in-the-wild malware using the investigated devices.